Electronic Frontiers
AUSTRALIA

PO Box 1302, Kensington VIC 3031
T +61 3 9013 9492 F +61 3 9013 9468
E email@efa.org.au W www.efa.org.au
ABN 35 050 159 188

Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001

Via email to: info@alrc.gov.au

13th November 2013

Dear Commissioners,

Submission to review of Serious Invasions of Privacy in the Digital Era

Electronic Frontiers Australia (EFA) welcomes this opportunity to make a submission in relation to the review of Serious Invasions of Privacy in the Digital Era. EFA acknowledges and thanks the Australian Privacy Foundation for its assistance in drafting this submission.

About EFA

Established in January 1994, Electronic Frontiers Australia, Inc. (EFA) is a national, membership-based non-profit organisation representing Internet users concerned with on-line freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of computer based communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems.

EFA's website is at: www.efa.org.au.

Yours sincerely,

Jon Lawrence, Executive Officer
Phone: 0414 669 787
Email: jlawrence@efa.org.au

General remarks

EFA treats privacy as one aspect of a broad positive right to informational self-determination. As the late Professor of Public Law Alan F. Westin put it in *Privacy and Freedom (1970)*, this is "The right of the individual to decide what information about himself [sic] should be communicated to others and under what circumstances." Within this, privacy is a gestalt of personal choices around forms of information release and the accountability of institutions dealing with private information. As such, EFA strongly supports the introduction of legislation in the Commonwealth Parliament to establish a cause of action for serious invasion of an individual's privacy.

In today's increasingly digitalised world, the consequences of serious invasions of individual privacy can be immediate and global in scope and have the potential to inflict serious harm on affected individuals, from simple embarrassment, loss of employment, breakdown of relationships, to, in some circumstances, creating a genuine risk of suicide. There are currently few remedial options available to Australians affected by serious invasions of privacy, and the establishment of a cause of action in this context would address this deficit.

A cause of action for serious invasion of individual privacy would be a powerful signal that individual privacy is a right that should be respected. EFA believes that this signalling function is as important a benefit of the establishment of such a cause of action as the remedial effects of any damages that may result from the bringing any such action.

EFA believes that it is possible to establish such a cause of action without unduly inhibiting freedom of expression, and particularly the implied freedom of political communication as has been determined by the High Court. EFA also believes that the establishment of such a cause of action would not inhibit effective law enforcement activities nor intelligence and national security-related activities.

Further, the establishment of a cause of action for serious invasion of privacy in national legislation would address serious inconsistencies across Australia's various jurisdictions as well as providing potential redress for individuals affected by serious invasion of privacy on the part of organisations not covered by the current Privacy Act 1988.

Principles guiding reform

Question 1. What guiding principles would best inform the ALRC's approach to the Inquiry and, in particular, the design of a statutory cause of action for serious invasion of privacy? What values and interests should be balanced with the protection of privacy?

Response: As noted in our introduction, EFA considers informational self-determination to be the overall guiding principle by which privacy another other positive digital rights should be determined. EFA also broadly agrees with the principles set out in the ALRC's Issues Paper, namely:

- Privacy as a value
- Privacy as a matter of public interest

- The balancing of privacy with other values and interests
- International standards in privacy law
- Flexibility and adaptability
- Coherence and consistency
- Access to justice

And we would add:

- Accountability of content and process

EFA believes that, using informational self-determination as guiding meta-principle, these other principles should be considered equally important and that no one principle should be seen as more important than any other. Interpretation and application of these principles should therefore be undertaken on a holistic basis.

The impact of a statutory cause of action

Question 2. *What specific types of activities should a statutory cause of action for serious invasion of privacy prevent or redress? The ALRC is particularly interested in examples of activities that the law may not already adequately prevent or redress.*

Response: EFA believes that it is appropriate for a non-exhaustive list of examples of the types of invasions that fall within the cause of action to be included in legislation establishing that cause of action. The examples provided in the ALRC's Issues Paper (as listed below) are appropriate and provide a useful starting point for such a non-exhaustive list of examples:

- there has been an interference with an individual's home or family life;
- an individual has been subjected to unauthorised surveillance;
- an individual's correspondence or private, written, oral or electronic communication has been interfered with, misused, or disclosed; or
- sensitive facts relating to an individual's private life have been disclosed.

Passive surveillance, through the use of new technologies such as drones or wearable devices, such as Google Glass, is another example of an activity that may not be adequately addressed under current laws but which may fall within the scope of a cause of action for serious invasion of privacy.

EFA also believes that there should be consideration of whether aggregated details of an individual's location over a period of time would be considered an act of unauthorised surveillance, and , further, whether such information would be considered as sensitive facts relating to an individual's private life.

Question 3. *What specific types of activities should the ALRC ensure are not unduly restricted by a statutory cause of action for serious invasion of privacy?*

Response: EFA believes that the ALRC should avoid specifying any types of activities that should be exempted from a statutory cause of action for serious invasion of privacy. Activities that may be considered, *prima facie*, to be legitimate such as law enforcement or

intelligence gathering relating to national security, can be covered by a 'public interest' defence. However, EFA would argue that the standard for this defence needs to be very high given the sensitivity of personal information. Activities that collect and make use of private information must be proportionate, necessary, and reasonable. They must be subject to processes of accountability, including judicial and parliamentary oversight where necessary. And, finally, there must be inspectable decision paths sufficient to prevent abuse or to ensure that abuse can be traced after the fact.

Invasion of privacy

Question 4. *Should an Act that provides for a cause of action for serious invasion of privacy (the Act) include a list of examples of invasions of privacy that may fall within the cause of action? If so, what should the list include?*

Response: EFA believes that it is appropriate for such an Act to include a list of examples, provided that any such list is explicitly non-exclusive nor exhaustive. It is critical that any Act establishing a cause of action for serious invasion of privacy retain maximum flexibility for courts to consider situations that fall outside the scope of the list of examples provided. Rather than provide our own full non-exhaustive list, we provide below three 'categories' of examples that should be included. Again, these are non-exhaustive, but they cover major areas of concern.

One very important set of examples will need to cover data breaches from all forms of institutions and corporations, where through deliberate or accidental process or actions the personal data of online site users is lost, stolen, or shared in a manner not consented to by the users. Regardless of whether that data is published or not, the fact of a data breach can have consequences from the embarrassing to the catastrophic.

A second set of examples will need to cover aggregated collections of data. These will include physical locational data from GPS units, mobile telephony, and technologies yet to be invented. These will also include virtual data such as search histories and histories of website or app use. The issue here is that both individual moments and aggregated moments can lead to severe intrustions of privacy. This is especially the case if aggregated data is sold or given from the original aggregator to third parties.

Finally, a third set of examples should cover the increasingly common online posting of photographs, audio-recordings, and video-recordings of personal spaces, activities, and bodies for which consent to post has not been expressly provided by the participant or all participants in dyadic or larger groups. This is intended to cover the posting or re-posting of so-called "revenge-porn" (posting sexual acts by one partner without the consent of the other/others after the dissolution of a relationship) and other voyeuristic images (pornographic or not). There is, of course, a difficulty here with also allowing consenting adults to enter into informal contracts to either view or post photographs, audio-recordings, and video-recordings of personal spaces, activities, and bodies.

Question 5. *What, if any, benefit would there be in enacting separate causes of action for:*

- *misuse of private information; and*
- *intrusion upon seclusion?*

Response: EFA believes that a single, flexible cause of action is preferable, rather than separate causes, to ensure that all possible situations are catered for.

Privacy and the threshold of seriousness

Question 6. *What should be the test for actionability of a serious invasion of privacy? For example, should an invasion be actionable only where there exists a 'reasonable expectation of privacy'? What, if any, additional test should there be to establish a serious invasion of privacy?*

Response: EFA agrees with the proposal that a privacy invasion should have two parts: a 'reasonable expectation of privacy' and some form of demonstrable act of consent by the participant to opt in or opt out (as the case may be) of sharing personal information. These should be flexible notions to be interpreted by courts on a case-by-case basis, thereby allowing for social and technological changes.

EFA believes that any other tests to be applied to establish actionability should focus on the act of invasion itself. Tests should not focus on the nature and degree of harm. Focusing on harm negates privacy as a positive right of self-determination.

Privacy and public interest

Question 7. *How should competing public interests be taken into account in a statutory cause of action? For example, should the Act provide that:*

- *competing public interests must be considered when determining whether there has been a serious invasion of privacy; or*
- *public interest is a defence to the statutory cause of action?*

Response: EFA believes that courts should be required to consider the 'public interest' in a comprehensive sense, rather than considering that there are multiple, potentially competing 'public interests'. It is important, for example, that law enforcement activities or media interests should not be prioritised over the individual's right to privacy.

EFA does however believe that 'public interest' should be available as an affirmative defence to a statutory cause of action, provided that it is clear that 'public interest' involves a definable and substantive public 'good', and is not simply used as a cover for ratings-driven media curiosity, or potentially unnecessary law enforcement activities. The burden of proof in establishing the public interest should fall on the defendants.

Further, as noted above, EFA would argue that the standard for this defence needs to be very high given the sensitivity of personal information. Activities that collect and make use of private information must be proportionate, necessary, and reasonable. They must be subject to processes of accountability, including judicial and parliamentary oversight where necessary. And, finally, there must be inspectable decision paths sufficient to prevent abuse or to ensure that abuse can be traced after the fact.

Question 8. *What guidance, if any, should the Act provide on the meaning of 'public interest'?*

Response: As per the response to Question 7 above, EFA believes that the meaning of 'public interest' must include a definable and substantive public 'good'. It should be explicit that public curiosity, or 'newsworthiness', is not in itself a public 'good'.

Fault

Question 9. *Should the cause of action be confined to intentional or reckless invasions of privacy, or should it also be available for negligent invasions of privacy?*

Response: Negligent invasions of privacy are likely to be as damaging to the affected persons as intentional or reckless invasions, and in many cases may be more damaging. Indeed, data breaches (as discussed above) are often the result of negligence. The cause of action should therefore be available for intentional, reckless and negligent invasions of privacy.

Damage

Question 10. *Should a statutory cause of action for serious invasion of privacy require proof of damage or be actionable per se?*

Response: EFA believes that the cause should be actionable per se. As noted above, focusing on harm negates privacy as a positive right of self-determination. This would establish a clear deterrent regardless of the status, resources and resilience of the subject of that invasion. Any requirement for proof of damage would also likely favour well-resourced potential defendants (such as large media organisations) by creating an unnecessary burden on potential litigants.

Question 11. *How should damage be defined for the purpose of a statutory cause of action for serious invasion of privacy? Should the definition of damage include emotional distress (not amounting to a recognised psychiatric illness)?*

Response: EFA believes the definition of damage should be relatively broad, and should definitely include emotional distress, as well as embarrassment and humiliation.

Defences and exemptions

Question 12. *In any defence to a statutory cause of action that the conduct was authorised or required by law or incidental to the exercise of a lawful right of defence of persons or property, should there be a requirement that the act or conduct was proportionate, or necessary and reasonable?*

Response: EFA believes that a requirement for a test that establishes whether an invasive action defended on the basis stated above was proportionate, or necessary and reasonable is absolutely essential.

Without such a test, there is a real danger, if not even likelihood, of a statutory cause of action for serious invasion of privacy being fundamentally undermined as a result of

legislation that may invoke national security, law and order, or other justifications to authorise the unrestricted invasion of privacy by state agencies.

EFA believes that the courts are best placed to determine, on a case-by-case basis, whether any serious invasion of privacy by law enforcement, intelligence or other state agencies can be justified by applying a proportionate, or necessary and reasonable test.

Question 13. *What, if any, defences similar to those to defamation should be available for a statutory cause of action for serious invasion of privacy?*

Response: In the interests of ensuring freedom of expression, EFA believes it would be appropriate for specific defences relating to absolute privilege (for parliamentary and judicial proceedings) and to qualified privilege (for fair and accurate reports of proceedings of public concern) to apply to a statutory cause of action for the protection of privacy. Any other 'defamation defences' are likely to be covered by a broader 'public interest' defence.

Question 14. *What, if any, other defences should there be to a statutory cause of action for serious invasion of privacy?*

Response: None.

Question 15. *What, if any, activities or types of activities should be exempt from a statutory cause of action for serious invasion of privacy?*

Response: EFA is not aware of any activities, or types of activities, that should be exempt from a statutory cause of action for serious invasion of privacy. Legitimate and proportionate law enforcement and intelligence activities would be covered under the public interest defence, and as per the response to question 13 above, specific defences covering absolute and qualified privilege should ensure that freedom of expression is not unduly compromised.

Monetary remedies

Question 16. *Should the Act provide for any or all of the following for a serious invasion of privacy:*

- *a maximum award of damages;*
- *a maximum award of damages for non-economic loss;*
- *exemplary damages;*
- *assessment of damages based on a calculation of a notional licence fee;*
- *an account of profits?*

Response: EFA believes that courts should have significant flexibility in relation to the awarding of monetary damages, to ensure that penalties appropriate and proportionate to the damage caused and to the ability of the defendant to pay can be awarded.

Injunctions

Question 17. *What, if any, specific provisions should the Act include as to matters a court must consider when determining whether to grant an injunction to protect an individual from*

a serious invasion of privacy? For example, should there be a provision requiring particular regard to be given to freedom of expression, as in s 12 of the Human Rights Act 1998 (UK)?

Response: EFA believes that in practice it would be simpler and more efficacious to incorporate in the Act an explicit reference to freedom of political communication, both civil and criminal, in relation to the requirement for judicial consideration of public interest (Q7 above).

Other remedies

Question 18. *Other than monetary remedies and injunctions, what remedies should be available for serious invasion of privacy under a statutory cause of action?*

Response: EFA believes that an apology should be included as a potential remedy, in addition to, or in place of monetary damages, depending on the wishes of the litigant.

Who may bring a cause of action

Question 19. *Should a statutory cause of action for a serious invasion of privacy of a living person survive for the benefit of the estate? If so, should damages be limited to pecuniary losses suffered by the deceased person?*

Response: EFA believes that a statutory cause of action for a serious invasion of privacy should survive for the benefit of the estate in the case of the death of the subject. The same remedies should be available to the estate as to the living person.

Question 20. *Should the Privacy Commissioner, or some other independent body, be able to bring an action in respect of the serious invasion of privacy of an individual or individuals?*

Response: EFA believes that the Privacy Commissioner, or other appropriate independent body, should be able to bring an action in respect of the serious invasion of privacy of an individual or individuals. Any such action should not preclude the individual/individual's ability to pursue an action themselves.

Limitation period

Question 21. *What limitation period should apply to a statutory cause of action for a serious invasion of privacy? When should the limitation period start?*

Response: EFA believes a one year limitation period is appropriate, starting from the point at which the subject becomes aware of the invasion of their privacy.

Location and forum

Question 22. *Should a statutory cause of action for serious invasion of privacy be located in Commonwealth legislation? If so, should it be located in the Privacy Act 1988 (Cth) or in separate legislation?*

Response: Particularly in the digital era, the consequences of invasions of privacy pay no respect to state, or even national borders. A statutory cause of action for serious invasion of privacy must therefore be located in Commonwealth legislation. Separate varying state-

based legislation in this context (as in so many other contexts), creates unnecessary duplication, uncertainty and inefficiency, and creates the potential for forum-shopping.

EFA believes separate legislation should be enacted to establish a statutory cause of action for serious invasion of privacy.

Question 23. *Which forums would be appropriate to hear a statutory cause of action for serious invasion of privacy?*

Response: EFA believes that the Federal Court is the appropriate forum to hear statutory causes of action for serious invasions of privacy.

Question 24. *What provision, if any, should be made for voluntary or mandatory alternative dispute resolution of complaints about serious invasion of privacy?*

Response: EFA believes that provision should be made for the voluntary use of alternative dispute resolution processes to deal with complaints about serious invasion of privacy, where both parties are in agreement. EFA does not believe that mandatory use of alternative dispute resolution is appropriate.

Interaction with existing complaints processes

Question 25. *Should a person who has received a determination in response to a complaint relating to an invasion of privacy under existing legislation be permitted to bring or continue a claim based on the statutory cause of action?*

Response: EFA believes a person in this situation should be permitted to bring or continue a claim based on the statutory cause of action. The courts can then decide whether there is a legitimate case to be heard. This permission would allow a person that is unsatisfied with a determination to attempt to seek satisfaction and should therefore play an important role in ensuring that the Office of the Australian Information Commissioner, or its successor, is responsive to the needs of subjects of serious invasions of privacy.

Other legal remedies to prevent and redress serious invasions of privacy

Question 26. *If a stand-alone statutory cause of action for serious invasion of privacy is not enacted, should existing law be supplemented by legislation:*

- *providing for a cause of action for harassment;*
- *enabling courts to award compensation for mental or emotional distress in actions for breach of confidence;*
- *providing for a cause of action for intrusion into the personal activities or private affairs of an individual?*

Response: EFA strongly believes that the enacting of a stand-alone statutory cause of action for serious invasion of privacy is the appropriate reform, and that incremental change to existing legislation, such as the items noted above, will be insufficient to deal with this increasingly important issue.

Question 27. *In what other ways might current laws and regulatory frameworks be amended or strengthened to better prevent or redress serious invasions of privacy?*

Response: EFA is concerned about the increase in sophistication, intrusiveness and pervasiveness of surveillance technologies and practices over recent decades.

State and Territory laws which are the most relevant to these issues are seriously inconsistent, are out-dated and are poorly enforced. EFA believes that the terms of reference of this review allow the ALRC to review, and recommend changes to address the inconsistent and inadequate State and Territory regimes that regulate surveillance technologies and practices.

EFA believes the ALRC should take the following issues into account when performing this review:

- whether it is desirable to introduce a uniform, national regime, and the means available to the Commonwealth for promoting consistency among the States and Territories;
- the need to strengthen the State and Territory regimes;
- whether it is desirable to introduce civil penalties, which may go some way towards redressing the inadequate enforcement of current criminal offences;
- the need for legislation to be updated to allow for effective regulation of new and emerging surveillance technologies;
- and in the absence of an effective regulator, the possibility of individuals bringing private actions to enforce breaches of surveillance devices laws.

Question 28. *In what other innovative ways may the law prevent serious invasions of privacy in the digital era?*

Response: EFA agrees with the following proposals, as provided to it by the Australian Privacy Foundation.

Protecting against serious invasions of privacy in a society that is increasingly characterised by the use of pervasive privacy-invasive and surveillance technologies, especially in the online context, cannot depend solely on law and regulation. There is a demonstrable need for holistic and concerted policies that promote education and privacy enhancing technologies, and incorporate appropriate assessment of privacy invasive technologies. All too often, government and regulatory responses to threats to privacy rights have been half-hearted, piecemeal and inconsistent.

Nevertheless, despite the limitations of legal solutions, laws can play a vital role in both inhibiting privacy invasions and in public education. An area of particular concern is the ready availability of affordable technologies that enable private individuals to collect, process and disseminate personal information on an industrial scale. This is particularly evident with the widespread use of social media, although it is not confined to those applications. The extent to which private individuals may increasingly engage in large-scale processing of personal information calls out for innovative legal and social strategies.

In its 2008 report on Australian privacy law, the ALRC rejected the view that the Privacy Act 1988 (Cth) should be extended to apply to individuals acting in a non-commercial capacity.

At that time, the Commission also rejected the possibility of establishing a take-down notice regime that would apply to online personal information. Acknowledging that a statutory cause of action would not adequately address the problems arising from the use and disclosure of personal information on the Internet, the ALRC confined itself to emphasising the importance of public education, especially in relation to the 'privacy aspects of using social networking sites'.

It should be noted that, since the ALRC's report, the use of social networking has become more pervasive and, accordingly, the privacy threats posed by social media have become more apparent.

In the light of these developments, EFA considers that the ALRC should revisit the conclusions reached in the 2008 report. In doing so, EFA believes that the current reference provides an opportunity for the ALRC to consider:

- the appropriate role of intermediaries, including social networking operators and search engine operators, in protecting online privacy.

In relation to serious invasions of privacy online, EFA considers that it is absolutely essential for the ALRC to give due consideration to the need for intermediaries, especially social networking service providers, but also search engine providers, to take appropriate responsibility for commercial services and activities which are premised on privacy invasions. This means that not only should the potential liability of intermediaries be considered in the context of innovative solutions to invasions of online privacy, but that full consideration should be given to the potential for intermediaries to be subject to secondary liability for breaches of any proposed statutory tort. If intermediaries were to be held secondarily liable for breaches of a statutory cause of action, EFA notes that there may be a case for a qualified defence that would limit liability where an intermediary takes reasonable steps to prevent privacy breaches, or limit the harms arising from online breaches.